

# WHAT IS CLAIMED IS:

1. A signature calculation system by use of a mobile agent, comprising: a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which  
5 can be visited by the mobile agent, wherein:

the base host includes:

an agent execution environment for letting the mobile agent execute its program code;

10 a random number generation means for generating random numbers;

a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means and a secret key of the owner of the mobile agent are inputted and which generates partial signature auxiliary data for distributing the  
15 information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts; and

20 a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means, and

each remote host includes:

25 an agent execution environment for letting the mobile agent execute its program code;

a partial signature calculation means to which signature target data, data which have been carried by the mobile agent and a secret key of the remote host are inputted and which calculates a partial

30 signature which is necessary for the calculation of the digital signature of the owner of the mobile agent;

a partial signature combining means to which one or more partial signatures calculated by one or more remote hosts are inputted and which outputs the digital signature calculated for the signature  
35 target data by use of the secret key of the owner of the mobile agent; and

a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature calculated by the partial signature calculation means, and

the mobile agent, which started from the base host carrying the  
40 partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the secret key of the owner of the mobile agent, and thereafter visits  $k$  ( $k$ : security parameter) remote hosts and  
45 carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the secret key of the owner of the mobile agent is obtained from the partial signatures calculated by the  $k$  remote hosts.

2. A signature calculation system by use of a mobile agent as claimed in claim 1, wherein one or more components of the remote host selected from the partial signature calculation means, the partial signature combining means and the public key cryptography calculation  
5 means are implemented by program code of the mobile agent.

3. A signature calculation system by use of a mobile agent as claimed in claim 1, wherein the partial signature auxiliary data generated by the partial signature auxiliary data generation means

include cipher texts  $(G_i, M_i)$  ( $1 \leq i < k$ ) which are obtained by  
 5 encrypting random numbers  $r_i$  ( $1 \leq i < k$ ) that satisfy a  
 predetermined relationship with the secret key of owner of the mobile  
 agent by use of ElGamal cryptosystem public keys  $y_i$  ( $1 \leq i < k$ ).

4. A signature calculation system by use of a mobile agent as  
 claimed in claim 3, wherein signatures calculated for the random  
 numbers  $r_i$  ( $1 \leq i < k$ ) by use of the secret key of the owner of the  
 mobile agent are added to the partial signature auxiliary data carried by  
 5 the mobile agent.

5. A signature calculation system by use of a mobile agent as  
 claimed in claim 1, wherein the digital signature calculated for the  
 signature target data is an RSA digital signature.

6. A signature calculation system by use of a mobile agent as  
 claimed in claim 5, wherein the partial signature combining means of the  
 remote host that presented the signature target data calculates the  
 digital signature for the signature target data by obtaining the product  
 5  $(\text{mod } p \times q)$  ( $p, q$ : prime number of approximately 512 bits)) of the partial  
 signatures calculated by the  $k$  remote hosts.

7. A signature calculation system by use of a mobile agent,  
 comprising: a mobile agent for calculating a digital signature of the owner  
 of the mobile agent; a base host of the mobile agent from which the mobile  
 agent starts moving in a network; and remote hosts in the network which  
 5 can be visited by the mobile agent, wherein:

the base host includes:

an agent execution environment for letting the mobile agent  
 execute its program code;

a random number generation means for generating random  
 10 numbers;

a partial signature auxiliary data generation means to  
 which the random numbers generated by the random number generation  
 means are inputted and which generates a new secret key and a new  
 public key corresponding to the newly generated secret key and generates  
 15 partial signature auxiliary data for distributing the information of the  
 newly generated secret key to the remote hosts so that the partial  
 signature auxiliary data will be used when partial signatures necessary  
 for the calculation of the digital signature of the owner of the mobile  
 agent are calculated by remote hosts; and

20 a public key cryptography calculation means for conducting  
 encryption and signature calculation for the partial signature auxiliary  
 data generated by the partial signature auxiliary data generation means,  
 and

each remote host includes:

25 an agent execution environment for letting the mobile agent  
 execute its program code;

a partial signature calculation means to which signature  
 target data, data which have been carried by the mobile agent and a  
 secret key of the remote host are inputted and which calculates a partial  
 30 signature which is necessary for the calculation of the digital signature of  
 the owner of the mobile agent;

a partial signature combining means to which one or more  
 partial signatures calculated by one or more remote hosts are inputted  
 and which outputs the digital signature calculated for the signature  
 35 target data by use of the newly generated secret key; and

a public key cryptography calculation means for conducting  
 encryption and signature calculation for the partial signature calculated  
 by the partial signature calculation means, and

the mobile agent, which started from the base host carrying the  
 40 partial signature auxiliary data and which is arbitrarily presented with  
 the signature target data by a remote host, stores the signature target  
 data if the mobile agent determined to write the digital signature for the  
 signature target data by use of the newly generated secret key, and  
 thereafter visits  $k$  ( $k$ : security parameter) remote hosts and carries the  
 45 partial signatures calculated by the remote hosts to the remote host that  
 presented the signature target data, at which the digital signature for the  
 signature target data by use of the newly generated secret key is obtained  
 from the partial signatures calculated by the  $k$  remote hosts.

8. A signature calculation system by use of a mobile agent as  
 claimed in claim 7, wherein one or more components of the remote host  
 selected from the partial signature calculation means, the partial  
 signature combining means and the public key cryptography calculation  
 5 means are implemented by program code of the mobile agent.

9. A signature calculation system by use of a mobile agent as  
 claimed in claim 7, wherein the partial signature auxiliary data  
 generated by the partial signature auxiliary data generation means  
 include cipher texts  $(G_i, M_i)$  ( $1 \leq i < k$ ) which are obtained by  
 5 encrypting random numbers  $r_i$  ( $1 \leq i < k$ ) that satisfy a  
 predetermined relationship with the newly generated secret key by use of  
 ElGamal cryptosystem public keys  $y_i$  ( $1 \leq i < k$ ).

10. A signature calculation system by use of a mobile agent as  
 claimed in claim 9, wherein signatures calculated for the random  
 numbers  $r_i$  ( $1 \leq i < k$ ) by use of a secret key of the owner of the mobile  
 agent, a signature calculated for the newly generated public key by use of  
 5 the secret key of the owner of the mobile agent, and the newly generated

public key are added to the partial signature auxiliary data carried by the mobile agent.

11. A signature calculation system by use of a mobile agent as claimed in claim 7, wherein the digital signature calculated for the signature target data is an RSA digital signature.

12. A signature calculation system by use of a mobile agent as claimed in claim 11, wherein the partial signature combining means of the remote host that presented the signature target data calculates the digital signature for the signature target data by obtaining the product  
5 (mod  $p \times q$  ( $p, q$ : prime number of approximately 512 bits)) of the partial signatures calculated by the  $k$  remote hosts.

13. A computer-readable record medium storing a program for instructing a computer of a base host of a mobile agent to execute:

an agent execution process for letting the mobile agent execute its program code;

5 a random number generation process for generating random numbers;

a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process and a secret key of the owner of the mobile agent as input data and  
10 generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts; and

15 a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature auxiliary

data generated in the partial signature auxiliary data generation process.

14. A computer-readable record medium storing a program for instructing a computer of a remote host to execute:

an agent execution process for letting a mobile agent execute its program code;

5 a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, data which have been carried by the mobile agent, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of  
10 the owner of the mobile agent for the signature target data;

a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of a secret key of the owner of the mobile agent; and

15 a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature calculated in the partial signature calculation process.

15. A computer-readable record medium as claimed in claim 14, wherein the digital signature calculated for the signature target data in the partial signature combining process is an RSA digital signature.

16. A computer-readable record medium as claimed in claim 15, wherein in the partial signature combining process, the digital signature for the signature target data is calculated by obtaining the product (mod  $p \times q$  ( $p, q$ : prime number of approximately 512 bits)) of the partial  
5 signatures calculated by the one or more remote hosts.

17. A computer-readable record medium storing a program for instructing a computer of a base host of a mobile agent to execute:

an agent execution process for letting the mobile agent execute its program code;

5 a random number generation process for generating random numbers;

a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process as input data, generating a new secret key and a new public key  
10 corresponding to the newly generated secret key, and generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are  
15 calculated by remote hosts; and

a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature auxiliary data generated in the partial signature auxiliary data generation process.

18. A computer-readable record medium storing a program for instructing a computer of a remote host to execute:

an agent execution process for letting a mobile agent execute its program code;

5 a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, data which have been carried by the mobile agent, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of  
10 the owner of the mobile agent for the signature target data;

a partial signature combining process for receiving one or more



partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of the newly generated secret key; and

- 15        a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature calculated in the partial signature calculation process.

19. A computer-readable record medium as claimed in claim 18, wherein the digital signature calculated for the signature target data in the partial signature combining process is an RSA digital signature.

20. A computer-readable record medium as claimed in claim 19, wherein in the partial signature combining process, the digital signature for the signature target data is calculated by obtaining the product (mod  $p \times q$  ( $p, q$ : prime number of approximately 512 bits)) of the partial  
5        signatures calculated by the one or more remote hosts.